REMARKS

Attached hereto is an Excess Claims Fee Letter for one excess total claim and one excess independent claim.

It is noted that the claim amendments herein are intended solely to more particularly point out the present invention for the Examiner, and not for distinguishing over the prior art or the statutory requirements directed to patentability.

It is further noted that, notwithstanding any claim amendments made herein, Applicant's intent is to encompass equivalents of all claim elements, even if amended herein or later during prosecution.

Claims 1-49 are all of the claims pending in the present Application. New claim 49 is added. Claims 1-3, 5, 6, 14, 20, 24-27, 30, 31, 35, 37, 39-45, 47, and 48 stand rejected under 35 USC §102(e) as anticipated by US Patent 6,219,439 to Burger. Claims 1, 2, 4, 14, 19-23, 28, 29, 35-44, 46, and 49 stand rejected under 35 USC §102(e) as anticipated by US Patent 6,038,315 to Strait, et al.

Applicants gratefully acknowledge the Examiner's indication that claims 7-13, 15-18, and 32-34 would be allowable if rewritten in independent format. However, Applicants believe that the independent claims, once properly understood, are currently allowable over the prior art of record and, therefore, respectfully declines to rewrite these claims in independent format at this time.

These rejections identified above are respectfully traversed in view of the following discussion.

I. THE CLAIMED INVENTION

As described and claimed, for example by claim 1, the present invention is directed to a method of authenticating a subject, including using one or a plurality of biometric measurements for authentication without any sharing of the subject's biometric data.

That is, unlike conventional systems, the present invention provides a technique in which the subject's biometric data is not exported from the device that stores the biometric data for the authentication process, since the device itself includes the comparison calculator.

A key advantage of the present invention is that the subject can be authenticated without an invasion of privacy (e.g., without sharing the biometric data with an external comparison device).

The prior art of record fails to teach or suggest this capability of preventing an invasion of privacy.

II. THE PRIOR ART REJECTION

The Examiner alleges that US Patent 6,219,439 to Burger anticipates claims 1-3, 5, 6, 14, 20, 24-27, 30, 31, 35, 37, 39-45, 47, and 48, and that US Patent 6,038,315 to Strait, et al. anticipates claims 1, 2, 4, 14, 19-23, 28, 29, 35-44, 46, and 49.

Applicants disagree, since both these conventional techniques have to share the biometric data in order to perform a comparison.

First, Burger relies on a reader 12, which is external to the smart card 14 that contains the biometric data, to compare the currently measured biometric scan with the data stored on the card (column 5, line 66 through column 6, line 1). Although there is no transmission needed in Burger, a subject's biometric privacy is not protected, since it is shared by the reader. That is, the reader 12 in Burger is not protected against even a simple security attack.

Additionally, since the fingerprint sensor 16 in Burger is incorporated into the reader 12, this biometric data from the sensor 16 is also subject to a security attack.

In contrast, as shown in Figure 1, the present invention includes a device 100 that contains not only the biometric data in non volatile storage 130, but also sensor(s) 110 and processor 120 that performs the comparison. Thus, the device 100 performs a comparison without having to share the biometric data stored therein with an external reader, such as used in Burger.

Hence, turning to the clear language of the claims, there is no teaching or suggestion of " ... without any sharing of the subject's biometric data."

Thus, independent claims 1, 37, and 39 are clearly patentable over Burger, and dependent claims 2-13, 38, and 40 are allowable if for no other reason than dependency.

Relative to independent claim 14, there is no teaching or suggestion of "... said subject maintaining confidentiality of authentication information and withholding said authentication information from any other party."

Thus, independent claim 14 and dependent claims 15-19 are clearly patentable over Burger.

Relative to independent claims 20 and 41, although Burger arguably has biometric information carried with the subject, it does teach or suggest an external application requests a password from a subject's authentication device, while simultaneously the subject's authentication device is interrogating biometric information from the subject. Therefore, independent claims 20 and 41 and dependent claims 21-34 and 42 are patentable over Burger.

Relative to claims 35, 37, and 43, Burger relies upon an external reader 12 and, therefore, does not teach or suggest "... a reader, associated with the subject, for reading a specified biometric of said subject ...."

Therefore, independent claims 35, 37, and 43, and dependent claims 36, 38, and 44-48 are patentable over Burger.

Second, the Examiner seems somewhat confused as to the significance of the encoding technique used in Strait. Although the Strait encoding technique might reasonably be considered as providing some protection of the biometrics reference from public access, in particular, a party who does not have access to the secret code word C. However, the system in Strait does have access to C and, therefore, the administrators of that system have access to the biometrics information. (e.g., as stated in column 2 at line 45, "... thereby recovering the original biometrics measurement taken ....") As a result, the subject's biometrics identity is known to the system's administrator. Therefore, the privacy protection in Strait is only against attacks from the outside but offers no privacy protection against internal complicity.

More important, Strait essentially concentrates on teaching a method of encoding biometric data, based on Hamming distance (see abstract), but fails to provide details as to how the hardware is actually implemented. That is, the encoding technique discussed in Strait does not at all ensure that sharing of biometric data is precluded. Indeed, it would appear that the description relied upon by the Examiner expressly describes an inherent sharing of biometric data.

More specifically, the Examiner points to lines 53-56 of column 2: "Conventional Diffie-Hellman public key encryption schemes and hashing procedures can then be used to secure the communications lines carrying the biometric information and to secure the database of authorized users." It is clear from this description that the biometric data in Strait is shared by the requester.

There is no reasonable interpretation that Strait provides the sensor, biometric data storage, and comparator on the same device, as done in the present invention, thereby precluding the sharing of the biometric data.

Therefore, independent claims 1, 37, and 39 are clearly patentable over Strait, and dependent claims 2-13, 38, and 40 are allowable if for no other reason than dependency.

Relative to claims 2 and 44, there is no suggestion at lines 47-55 of column 3 that the database is an individual unit belonging to the subject. Indeed, the above-cited lines 53-56 of column 2 suggest a database located remotely. It is noted that the Applicants interpret that the Examiner actually intended to refer to Strait, rather than Burger, on page 13 of the Office Action.

Relative to claims 14 and 39, the above-cited lines 53-56 of column 2 clearly describes that the biometric data is shared with the requester.

Relative to claim 20, the Examiner seems to consider "interrogating biometric information" in Strait as referring to the encoding execution of the input sensor. However, this biometric information is not carried by subject. Moreover, any "password" in Strait would have to be considered as derived from the sensed biometric information. Therefore, there is no simultaneous password request and interrogating biometric information, as required by the claim.

Relative to claims 21 and 41, the Examiner contradicts the "simultaneous" aspect of claim 20 in which the password is requested simultaneous with the interrogation of the biometric information.

Relative to claim 22, the above-cited lines 53-56 of column 2 clearly describes that the biometric data is shared with the requester. Therefore, Strait cannot reasonably be considered as withholding information so that the biometric is not revealed to a party requiring authentication. Clearly, the system performing the authentication process is

requiring this authentication and, clearly, this system has full access to the subject's biometric data.

Relative to claims 29 and 40, the lines cited by the Examiner (i.e., lines 5-64 of column 3) do not at all describe "... measuring a biometric-print of the subject by ranking biometric prints of N subsets of M biometrics ..." nor does it describe "... wherein an index of a top ranking of each of the N subsets is used in computing the password".

Relative to claim 35, the privacy of the subject is clearly compromised according to lines 53-56 of column 2, since the biometric data is clearly transmitted on communication lines.

Relative to claim 37, access to the biometric of the subject is clearly provided to someone other than the subject, according to lines 53-56 of column 2, since the biometric data is clearly transmitted on communication lines.

Relative to claim 42, the lines cited by the Examiner (i.e., column 3, lines 5-64) do not at all demonstrate "... a set of N best matches for N subsets, and an index formed by concatenation of the N indices uniquely identifies the subject."

Relative to claim 43, there is no "reader, associated with the subject" in Strait.

Relative to claim 48, the above-cited lines 53-56 of column 2 clearly describes that the subject's identity is determined at a remote location, since the biometric data is transmitted across communications lines. Nor does column 3 at lines 5-64 describe "... a set of N best matches for N subsets, and an index formed by concatenation of the N indices uniquely identifies the subject." It is presumed that the Examiner intended to refer to Strait, rather than Burger, on page 13 of the Office Action.

For the reasons stated above, the claimed invention is fully patentable over the cited references.

Further, the other prior art of record has been reviewed, but it too, even in combination with Burger and Strait, fails to teach or suggest the claimed invention.

IV. FORMAL MATTERS AND CONCLUSION

The Examiner objected to the spelling of "possession" in line 20 of page 2 of the specification. Applicants believe the specification amendment above addresses the Examiner's concern and requests that the Examiner reconsider and withdraw this objection.

The Office Action included a copy of the Draftsperson PTO 948 form. Applicants submit under separate cover a new set of formal drawings.

In view of the foregoing, Applicant submits that claims 1-49, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview. The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: 9/25/03

Frederick E. Cooperrider
Reg. No. 36,769

McGinn & Gibb, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, Virginia 22182
(703) 761-4100
Customer No. 21254